Certified True Randomness created by Cambridge Quantum Computing

Mission critical part of the process to safeguard communications in the quantum computing age developed by Cambridge Quantum Computing.

(Cambridge July 28th 2017)

Background

The generation of random numbers and sequences is a critical part of numerous computational processes that are vital across the world and across industries. Generating random numbers is the most critical aspect for any secure communications using quantum computing or quantum technological platforms – by definition, quantum keys cannot be developed without a secure source of true, device independent randomness.

Until now, classical random number generators are entirely deterministic. Even the most sophisticated method or programme for generating randomness relies on a pre-set algorithm or series of algorithms. Consequently, this output cannot be trusted without further assumptions that in turn undermine the process.

Since it is not possible to create randomness out of nothing random numbers generated by any sort of software are vulnerable to hacking or repetition.

Quantum mechanics is intrinsically probabilistic and therefore allows for the generation of randomness (for example sending a photon through a beam-splitter and measuring in which arm it ends up). However even here one must trust that the quantum devices are operating, as they should. True certifiable randomness requires a protocol that is device independent.

Cambridge Quantum Computing ("CQC") has answered a question that has challenged researchers for decades - is there a way of generating randomness in a device-independent and certifiable way?

Cambridge Quantum Computing's Invention

As recent headlines from around the world including China and Russia reinforce the inevitable move from digital to quantum-based communications, the very foundations of our encryption systems will need reviewing.

The most critical component in any quantum technology or quantum computing based communications methodology is the ability to generate random numbers. All quantum key distributions will require such basic ingredients.

There has, until now, been no true "certified" randomness in the world, and even primitive quantum mechanical based random number generators are not device independent or certified. Cambridge Quantum Computing has invented a certified true randomness generation protocol that is device independent.

The protocol, which the company refer to as "RNG", was invented by CQC's scientists Fernando Brandao (currently at Caltech) and Simone Severini (currently at UCL), and has been one of the core projects of Cambridge Quantum Computing.

The company said "Having spent a number of years perfecting the research basis for RNG, we are in the early stages of commercialising this essential technology that in many ways has for decades been the 'holy grail' for quantum communications".

The company continued, "For the first time in human history we have the ability to generate and use certified true randomness. CQC's protocol allows scaled use that will be the embedded key for all future quantum communications where randomness is required to be guaranteed and to be device independent. Applications ranging from national security to finance, and including communications from embedded devices and the 'internet of things' to basic fintech effectiveness will require RNG. In fact anyone who uses Monte-Carlo simulations will also require certified true randomness and will ultimately have to migrate from pseudo-random generating methods to secure truly random generators that are device independent"

About Cambridge Quantum Computing

Based in Cambridge and London, and with offices in Hong Kong and a presence in the United States, CQC is the leading independent quantum algorithm and quantum software company. In addition to the randomness protocol CQC has created a unique compiler (named "t|ket>") for quantum processors. CQC is also active in creating quantum algorithms that will drive value from early stage quantum processor with "shallow" circuits and has a focus here in two areas - firstly the analysis of complex time series and secondly on quantum chemistry.

More information can be found at www.cambridgequantum.com